GDPR White Paper

zscaler™

Cordery®
Legal.Compliance

Introduction

You'd need to live in a cave not to have 25 May 2018 etched into your memory. That's the go-live date of the General Data Protection Regulation (GDPR) the EU's comprehensive new data protection law. Many forests have been killed for GDPR articles. We don't want to add unnecessarily to that, but we want to set out a different view on some key aspects of GDPR. We're doing this by looking at the same issues from two different stand points – that of the seasoned CISO and that of the experienced data protection lawyer.

We use a few GDPR terms and abbreviations in this note. If you're not familiar with them, you can find out more details in Cordery's data protection glossary here.

With such an intrinsic link between data protection, data privacy and information security, it is easy to see why many GDPR readiness programmes are being driven by the CISO. Whilst this approach has its merits, the overwhelming majority of the requirements of GDPR are focused on areas which the CISO and their team are unable to influence.

What's it all about?

In the EU personal data can only be gathered under strict conditions and for legitimate purposes only – those who collect and manage people's personal information must protect it from misuse and must respect their rights. There are now more obligations, potential liabilities, expanded and new rights and significant penalties if you get it wrong. But GDPR isn't as scary as some people think – if you use the right technology and processes and train your people properly you'll meet many of GDPR's requirements.

The CISO lens on this one is easy – once the information has been identified and classified as 'personal data', the security function, in line with GDPR Article 32, can ensure that the processing of information is carried out in an appropriate fashion. The term 'secure' is subjective but the security function should ensure a standard set of controls commensurate with the sensitivity of information – as GDPR itself says, it's all about ensuring a level of security appropriate to the risk.

The CISO can provide tools to assist the business in identifying personal data. Encryption is a huge challenge in 2018. It is important that security controls exist that can inspect encrypted traffic flows to identify potentially sensitive information leaving the company perimeter!

©2018 Zscaler, Inc. All rights reserved.

Key concepts

By way of a quick reminder some of the key concepts of GDPR are as follows:

What is personal data?

Personal data is data relating to a living individual who can be identified from that data, either alone or with other information in a data controller's possession – GDPR defines personal data very widely, and more extensively than the US PII definition. There is also sensitive personal data which under GDPR consists of information relating to racial or ethnic origin, political or religious beliefs, trade union membership, the processing of genetic and biometric data to identify an individual, health, sex life or sexual orientation – under GDPR this is now referred to as special category data. Information relating to criminal offences still receives special treatment under GDPR too.

The CISO earns their paycheck by helping business stakeholders identify data elements that could be considered 'personal'. Given GDPR's broad interpretation, often there are things which are simply overlooked as being 'personal' – Cookies, digital certificates, IP addresses, etc. Not in all cases but when combined with other elements they build up a personal picture of a data subject.

What are data controllers and processors?

A data controller is any person or entity who determines how and for what purposes personal data is processed – a third party may carry out processing on the controller's behalf, although the data controller remains responsible for the processing. A data processor is a person or entity who processes personal data for a data controller, other than the controller's employee – outsourced IT service providers for example might be processors. Under GDPR the distinction between controllers and processors becomes a bit more blurred as processors take on more obligations and potential liability.

This is key for Zscaler – companies need to understand that when they're using cloud service providers (CSPs), they are generally doing so with the CSP being a 'processor'. The customer retains the control of the 'purpose and means' of their data and therefore they're the controller.

What is data processing?

Data processing is also a very wide concept encompassing just about everything that you can do with data including obtaining, recording, holding, organisation, alteration, retrieval, use, disclosure and blocking or destruction – most operations in relation to personal data will constitute processing.

©2018 Zscaler, Inc. All rights reserved.

What are anonymization and pseudonymisaton?

Anonymisation and pseudonymisation of personal data also constitute processing. Anonymisation is a method of processing personal data in order to irreversibly prevent identification – organisations try and anonymise data to make it more secure and to help them comply with their data protection responsibilities. Pseudonymisation is often confused with anonymisation but with pseudonymisation the individual can still be identified – for example at its most basic level changing an employee's name to an identification number instead and removing all of their other personal details could be pseudonymisation. The EU Article 29 Working Party in its paper on anonymisation has warned of the dangers of confusing pseudonymisation and anonymization saying that "pseudonymisation is not a method of anonymisation. It merely reduces the linkability of a data set with the original identity of a data subject, and is accordingly a useful security measure". It's a distinction that is important – truly anonymised data isn't subject to GDPR; pseudonymised data is. But in these days of data being connected at the blink of an eye truly anonymised data is becoming increasingly rare.

From the CISO's viewpoint a challenge will be the conflicting views of 30 years in technology with GDPR requirements – forever we have been using relational database management systems and file stores which were built to centralise information and make data matching and traceability straightforward – now we must undo not only technical solutions but educate into a profound mindset change pertaining to data storage.

An approach Zscaler uses is Nanolog architecture for backend storage – Nanolog is not a relational database and it is written with principles of minimisation and pseudonymisation in mind.

©2018 Zscaler, Inc. All rights reserved.

What are the Data Protection Principles?

GDPR sets out six principles (which interlink with each other) which in brief are as follows:

- **Lawfulness, Fairness and Transparency** – this means making sure that personal data is processed lawfully, fairly and transparently;
- **Purpose limitation** – this means that personal data can only be collected for specified, explicit and legitimate purposes;
- **Data minimisation** – this means making sure that use of personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) for which the data is being processed;
- **Accuracy** – this means making sure that data is accurate and, where necessary, kept up to date;
- **Storage limitation** – this means that data mustn't be kept for longer than necessary;
- **Integrity and Confidentiality** – this means making sure that personal data is processed in a manner that ensures the appropriate security of personal data, including protection against unauthorised or unlawful data processing and against accidental loss, destruction or damage.

The six principles really highlight the importance of having assigned data ownership in the organisation – business stakeholders who understand the 'why and what' of data collection and retention.

What is privacy by design and default?

GDPR has introduced a new concept called data protection by design and default. In simple terms this means that from the very start of activities touching on data processing privacy issues must be addressed. In more technical terms GDPR says that, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks that may be faced by individuals posed by the processing in question, a data controller must at the time of the determination of the means for processing and at the time of the processing itself implement appropriate technical and organisational measures.

The practical upshot is that data controllers will have to implement appropriate

©2018 Zscaler, Inc. All rights reserved.

technical and organisational measures for data processing, such as pseudonymisation in order to implement data protection principles such as data minimisation. Controllers will have to implement appropriate measures to ensure that, by default, only personal data which is needed for each specific purpose of the processing is processed – this will encompass the amount of personal data collected, the extent of their processing, the period of their storage, and, their accessibility. The measures must also ensure that by default personal data are not made accessible without an individual's intervention to an indefinite number of natural persons.

The security function can help here by ensuring that organisational project processes allow for security engagement to begin at project inception. It is no good having the security function involved after decisions have been made pertaining to data privacy and system design.

What about security and data breaches?

Under GDPR personal data has to be kept secure – this is probably the biggest risk issue of all for all organisations. Both data controllers and data processors have to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. In terms of assessing the appropriate level of security the risks presented by processing must be considered, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Generally-speaking a data breach is any data security issue which exposes (or could expose) personal data – under GDPR data breaches are defined widely. If there is a data breach (or a suspected one) it must usually be reported to a data protection regulator within 72 hours of first awareness of the breach. In the event of a data breach key objectives should be to: prevent the further spread/loss of data; recover the data that has been lost; identity risks arising from the breach; contact appropriate parties – GDPR states that it may also be necessary to inform the individuals who have been affected by a breach of the breach; and, prevent future breaches. Given the tight reporting deadline it will be imperative to act quickly with all aspects of handling a data breach.

Let us think about the steps involved in a data breach and the need for assimilating information swiftly. This is where the power of a platform architecture can come into play. Solutions such as the Zscaler™ Cloud Security Platform allow for a 'single pane of glass' view of reporting within our admin console. A good CSP will also offer the capability to stream important telemetry to a customer analytics platform/SIEM as needed.

©2018 Zscaler, Inc. All rights reserved.

Data Privacy Impact Assessments – a key compliance process

A Data Privacy Impact Assessment (DPIAs) is a process to identify data protection and privacy risk. Under GDPR, where processing operations present specific risks to (in effect) individuals' privacy rights due to their nature, scope or purposes, controllers, or processors acting on the controller's behalf, are to carry out an assessment of the impact of the proposed processing operations on the protection of personal data. In some cases DPIAs will be mandatory, notably where a type of processing in particular using new technologies is likely to result in a high risk to individuals' rights and freedoms. But it may be better to consider carrying out a DPIA as part of any new project involving personal data as a best practice.

A DPIA therefore aims to establish whether there might be any such risks – if there are any they will ultimately have to be addressed. Another important compliance obligation might also arise where a DPIA suggests that the processing in question would result in high risks which can't be mitigated. If this is the case a data protection regulator must then be consulted.

The "high risks" referred to above are not defined in GDPR, although EU regulatory guidance does attempt to set up a methodological approach to this to some degree. GDPR does however identify particular circumstances in which undertaking a DPIA is required in particular, which is based on factors such as systematic and extensive evaluation of personal data, or, processing on a large-scale of especially sensitive data. Data protection regulators may also develop criteria for processing operations for which DPIAs will be required.

Generally-speaking, a DPIA is conducted at the start of a project that could have data protection or privacy implications, e.g. rolling out a new document management system or a new product, or, making changes to the HR system. Official EU guidance suggests however that in some circumstances existing processes must also be reviewed. Although DPIAs will work best on a new project, they should also be used, either when you are planning material changes to an existing system, or to review an existing system, so long as there is a realistic opportunity to change the existing system.

It is probably best to use a template to help make the DPIA process consistent which should be added to where there are additional risks. DPIAs should also be signed off at an appropriate level, e.g. by the business lead.

Consultation is an important part of a DPIA and can take place at any point in the process, i.e. initial internal consultation before consulting a data protection regulator (if needed).

It is also important to remember that doing a DPIA is an ongoing process and so as any project develops new risks might be identified but equally ways to avoid risk might be found.

©2018 Zscaler, Inc. All rights reserved.

DPIAs sound daunting but if you follow a sound process you'll be able to spot risks and address them. Don't forget that your vendors should help you with this process too and choosing vendors with external accreditation like ISO 27001 can make the process easier.

It is also important to bear in mind that a key theme of GDPR is the requirement to formally document compliance and also demonstrate compliance (so-called accountability) - DPIAs very much fit in with this too. Remember that under GDPR data protection regulators have inspection powers – they can come onto premises looking for documents including DPIAs.

What rights are there under GDPR?

Individuals have a number of possible rights that they can exercise with regard to the personal data held on them as follows:

Subject Access Rights (SARs) – here an individual can seek to obtain confirmation as to whether or not personal data concerning them is being processed by a data controller, where and for what purpose, and to be provided with a copy of that personal data usually free of charge within a month – this is the right to most watch out for;

The Right to be Forgotten (data erasure) – here an individual can seek to have personal data held on them by a data controller erased, subject to certain conditions such as the data no longer being relevant to the original purpose for processing, or where an individual has withdrawn their consent to processing that data – this right can also be expected to be used frequently;

The Right to Rectification – here an individual can seek to have personal data that is held on them by a data controller corrected without undue delay where the data concerning them is inaccurate;

The Right to Restriction – here an individual can seek to restrict a data controller processing the personal data held on them by the controller, subject to certain conditions such as where the individual contests the accuracy of the data held on them for a period enabling a controller to verify the accuracy of the data in question;

The Right to Object to Processing – here an individual can seek to object to processing personal data held on them by a data controller on grounds relating to their particular situation where certain conditions apply such as where the lawful basis on which their data is being processed is so-called "legitimate interests" (as opposed to e.g. consent), including profiling. Where personal data are processed for direct marketing purposes, an individual also has the right to object at any time to processing of personal data concerning them for marketing, which includes profiling to the extent that it is related to direct marketing. Also an individual can seek to not be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them;

©2018 Zscaler, Inc. All rights reserved.

The Right to Portability – here an individual can receive the personal data concerning them which they have previously provided to a data controller in a structured, commonly used and machine-readable format and have that data transmitted to someone else, subject to certain conditions such as where the individual consented to the data controller processing their data.

It is important when assessing cloud providers that you understand their processes associated with the rights of data subjects. At Zscaler, we provide our customers (controllers) with a Data Processing Agreement. This covers the steps Zscaler take to ensuring that data pertaining to EU citizens can be deleted, restricted and/or reported on – using the right technology makes the process highly efficient (if you consider the alternative of trying to do this all manually you'll quickly realise the possible magnitude of the task in terms of time and resource).

Sanctions, liability and compensation

Under the new rules, data protection regulators have the power to impose high fines for infringing the new rules. Different bands of fines can be applied in relation to three different sets of categories of infringements – the highest level of fine is either a maximum of €20 million or 4% of the global annual turnover of a business, whichever is the greater.

As a general principle, any person who has suffered material or non-material damage due to an infringement of GDPR has a right to compensation from the data controller or processor concerned for the damage suffered, subject to various defences.

But its not all about fines – regulators have other powers too including ordering temporary or permanent holds on data processing.

Mandatory audits and dawn raids

Under the new rules regulators may carry out investigations in the form of data protection audits, and, they may obtain access to any premises of the controller and the processor, including to any data processing equipment and means. This may prove to be a significant tool in the data protection regulators' armoury.

©2018 Zscaler, Inc. All rights reserved.

Why Zscaler for GDPR?

GDPR requires an organisation to understand where it is storing and processing personal information of EU citizens. No vendor solution is going to provide GDPR compliance but technical solutions, with the correct implementation, can assist the CISO and Data Protection Officer in identifying the flows of personal information.

When looking at technical solutions within a GDPR context, it is important to think about several GDPR Articles and consider how your existing security architecture will be able to provide controls which satisfy the GDPR Article 32 requirements.

Is your organisation currently inspecting encrypted internet traffic? Almost all CSPs are offering SSL / TLS communication by default. If you are concerned about a lack of personal data visibility, you need to inspect encrypted traffic flows. Do you currently have a consistent technical security posture across your datacenter and branch office locations? All too often, best-of-breed security controls are deployed within the datacentre, leaving satellite locations with a downgraded security posture and a single appliance trying to operate as a proxy server, firewall and a router.

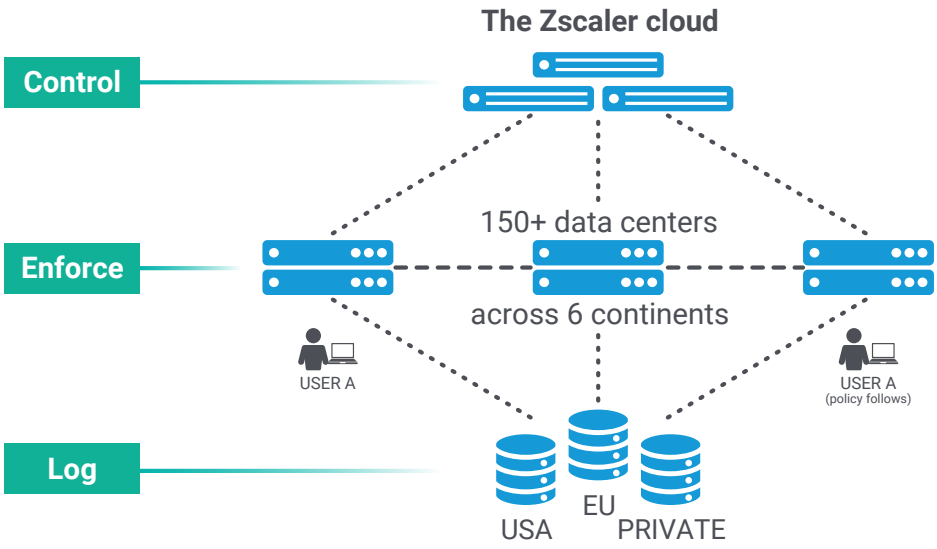
The GDPR 72-hour reporting window is another key consideration for the CISO. In a world of cloud services and an eroded corporate perimeter, how is your organisation going to assimilate forensic information in the event of a data breach? The proliferation of appliances and cloud services is causing the CISO a visibility and operational headache. Organisations need to have centralised control of their security stack. Some hate the phrase 'single pane of glass' but we must be looking at technology solutions which offer an aggregated reporting window of the environment being managed.

A final point to consider is data residency and retention: for companies adopting public cloud services, is your CSP adhering to requirements surrounding privacy by design and data minimization? Many of the technology solutions we use today are based on a foundation of relational databases and file stores. The solutions we use today are invariably based on a concept of caching, data retention and tight-coupling. All principles which challenge GDPR requirements of privacy and data protection by design.

At Zscaler, we take a different approach to web security. Our security controls are built into a unified platform, so they communicate with each other to give you a cohesive picture of all the traffic that's moving across your network. Through a single interface, you can gain insight into every request — by user, location, and device around the world — in seconds.

Zscaler takes its responsibilities as a data controller and a data processor very seriously. It all starts with our architecture. Zscaler built from scratch an infinitely scalable, cost-effective, and ultra-fast cloud security architecture that integrates three key components for control, enforcement, and logging: the Central Authority (CA), ZIA Public Service Edge, and Nanolog Servers.

©2018 Zscaler, Inc. All rights reserved.



Privacy protection at the Web Transaction level

- The ZIA Public Service Edge never stores any web transaction content or personal data
- Web transaction content is never written to disk; all content inspection takes place in memory
- Customer transaction logs (customer logs) are transferred to Zscaler Nanolog clusters in an encrypted format
- Customer logs are only available via the Zscaler web user interface by authorized administrators with appropriate privileges
- User identifiers can be obfuscated within Zscaler's web user interface

Privacy protection at the Facilities level

- Security standards on par with world-class financial and data centers for hub facilities (ISO27001, SOC 2 Type 2, or similar local certification)
- Authorized personnel must pass through multiple levels of security and biometric scanning to gain access
- All data centers are hosted in secure telecommunications centers at major internet exchange points globally
- 24x7x365 security management and site access via security operations center

Privacy protection at the Network level

- Customer logs are never stored in clear text
- Customer logs are transmitted as indexed, compressed and differential logs
- A single log is meaningless without a complete string of historic logs
- All communications between a ZIA Public Service Edge and a Nanolog cluster are encrypted using TLS

©2018 Zscaler, Inc. All rights reserved.

Watch the video – **GDPR Readiness: Best Practices and Guidelines**[1]

[1]https://youtu.be/zEAbpvuvvWo

©2020 Zscaler, Inc. All rights reserved. Zscaler™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, and ZPA™ are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners. V.062220

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com